ПРАВОВІ ЗАСАДИ НАЦІОНАЛЬНОЇ БЕЗПЕКИ УКРАЇНИ

Яковюк Іван Васильович,
доктор юридичних наук, професор,
завідувач кафедри права Європейського Союзу,
Національний юридичний університет
імені Ярослава Мудрого,
Україна, м. Харків
e-mail: yakoviyk@ukr.net
Scopus Author ID: 57200072341
ORCID 0000-0002-8070-1645

Волошин Артем Павлович,
аспірант кафедри права Європейського Союзу,
Національний юридичний університет
імені Ярослава Мудрого,
Україна, м. Харків
e-mail: voloshyn8888@gmail.com
ORCID 0000-0002-3600-3778

Шовкун Антон Олексійович,
магістр Інституту підготовки
юридичних кадрів для СБУ,
Національний юридичний університет
імені Ярослава Мудрого,
Україна, м. Харків
e-mail: toni.shovkun@gmail.com
ORCID 0000-0002-5280-8066

doi: 10.21564/2414–990x.149.200028
УДК [343.72:004.738.5]:341.171(4–6ЄС)

ПРАВОВІ АСПЕКТИ ПРОТИДІЇ ФІШИНГУ: ДОСВІД ЄВРОПЕЙСЬКОГО СОЮЗУ

Кібербезпека все частіше розглядається як фундаментальна проблема держави, що комплексно зачіпає її безпеку і оборону, економіку, окремі сфери суспільного життя, зокрема енергетику, охорону здоров'я тощо. Надійна робота мереж передачі даних, комп'ютерних систем та мобільних пристроїв є обов'язковою умовою для ефективного функціонування держави і суспільства, життєдіяльності окремого індивіда. Надійність роботи ключових інформаційних систем загального користування залежить від багатьох чинників: кібератак, збою апаратного та програмного забезпечення, різного роду помилок. Суттєве зростання кількості інцидентів у кіберпросторі обумовлює необхідність системного аналізу джерел виникнення загроз, на перше місце серед яких виходить фішинг. Запровадження кримінальної відповідальності за фішинг ускладнено тим, що «фішинг» – це «парасолькове» поняття, яка охоплює низку розпочатих чи завершених злочинів. Фішинг-атаки з точки зору кримінального права можуть відповідати різним категоріям злочинів (вимагання, шахрайство, шантаж, правопорушення, що пов'язані з обробкою персональних даних тощо). Спроба окремих держав запровадити кримінальне покарання за фішинг на національному рівні не вирішує проблему, оскільки для фішерів, які працюють по всьому світу, нескладно обійти національні бар'єри. Саме тому протидія кіберзлочинності потребує значних зусиль не лише окремих держав, але й міжнародних організацій, зокрема Європейського Союзу.

Ключові слова: кіберпростір; кібербезпека; кіберзлочинність; онлайн-шахрайство; фішинг; антифішингові інструменти; кримінальне право; Європейський Союз.

Яковюк И. В., доктор юридических наук, профессор, заведующий кафедрой права Европейского Союза, Национальный юридический университет имени Ярослава Мудрого, Украина, г. Харьков.
e-mail: yakoviyk@ukr.net ; Scopus Author ID: 57200072341 ; ORCID 0000-0002-8070-1645

Волошин А. П., аспирант кафедры права Европейского Союза, Национальный юридический университет имени Ярослава Мудрого, Украина, г. Харьков.
e-mail: voloshyn8888@gmail.com ; ORCID 0000-0002-3600-3778

Шовкун А. А., магистр Института подготовки юридических кадров для СБУ, Национальный юридический университет имени Ярослава Мудрого, Украина, г. Харьков.
e-mail: toni.shovkun@gmail.com ; ORCID 0000-0002-5280-8066

Правовые аспекты противодействия фишингу: опыт Европейского Союза

Кибербезопасность все чаще рассматривается как фундаментальная проблема государства, которая комплексно затрагивает его безопасность и оборону, экономику, отдельные сферы общественной жизни, в частности энергетику, здравоохранение и другие. Надежная работа сетей передачи данных, компьютерных систем и мобильных устройств является обязательным условием для эффективного функционирования государства и общества, жизнедеятельности отдельного индивида. Надежность работы ключевых информационных систем общего пользования зависит от многих факторов: кибератак, сбоя аппаратного и программного обеспечения, различного рода ошибок. Существенный рост количества инцидентов в киберпространстве обусловливает необходимость системного анализа источников возникновения угроз, первое место среди которых занимает фишинг. Введение уголовной ответственности за фишинг затруднено тем, что «фишинг» – это «зонтичное» понятие, которое охватывает ряд начатых или завершен-

ных преступлений. Фишинг-атаки с точки зрения уголовного права могут соответствовать различным категориям преступлений (вымогательство, мошенничество, шантаж, правонарушения, связанные с обработкой персональных данных и т.д.). Попытка отдельных государств ввести уголовное наказание за фишинг на национальном уровне не решает проблему, поскольку для фишеров, которые работают по всему миру, несложно обойти национальные барьеры. Именно поэтому противодействие киберпреступности требует существенных усилий не только отдельных государств, но и международных организаций, в частности Европейского Союза.

Ключевые слова: киберпространство; кибербезопасность; киберпреступность; онлайн-мошенничество; фишинг; антифишинговые инструменты; уголовное право; Европейский Союз.

Постановка проблеми. Стрімке розширення загроз національній безпеці у XXI ст. покладає на органи держаної влади завдання щодо їх попередження, виявлення та нейтралізації. Серед найбільш небезпечних загроз для України — кіберзлочинність, яка реалізується через мережу Інтернет. І це зрозуміло. На сучасному етапі і у подальшій перспективі розвиток як окремих суспільств і держав, так і загалом світу буде здійснюватися відповідно до концепції інформаційного суспільства, що пов'язана з використанням інформаційних і телекомунікаційних технологій у придбанні, зберіганні та обробці інформації у повсякденному житті [2; 42].

Актуальність нашого дослідження обумовлена вразливістю кіберпростору[1] та його базової інфраструктури до різного роду кібератак (порушення корпоративної безпеки, фішинг, вимагання в соціальних мережах тощо), які перетворилися на одну з найнебезпечніших загроз для особистої, національної, регіональної і глобальної безпеки. Так, станом на 2012 р. кібератаки коштували 114 мільярдів доларів США щороку, а з урахування часу, витраченого на відновлення нормальної роботи на усунення, загальна вартість кібератак досягне приголомшливих 385 мільярдів доларів [34, с. 973]. Крім того, слід брати до уваги, що оскільки кібератаки дешевші, зручніші та менш ризикові, ніж фізичні атаки, сьогодні в кіберпросторі вчиняється значна частка традиційних злочинів (виробництво та розповсюдження дитячої порнографії, банківські та фінансові шахрайства, порушення інтелектуальної власності, злочини з криптовалютою тощо), які спричиняють украй негативні гуманітарні, економічні та правові наслідки [46, с. 4017].

Кібербезпека більше не є проблемою виняткова комп'ютерної безпеки. У її забезпеченні зацікавлені усі держави, оскільки від її стану залежить, чи буде продовжувати ефективно функціонувати кіберпростір у ситуації кібератаки.

[1] Донедавна терміни з префіксом «кібер» мало вживалися в українському законодавстві. Натомість широко використовувалося поняття «інформаційна безпека». Від початку російсько-українського конфлікту у законодавстві почало застосовуватися як поняття «інформаційна безпека» («Доктрина інформаційної безпеки України», 2017) [24], так і «кібербезпека» («Стратегія кібербезпеки України», 2016) [59]. При цьому вказані акти не пояснюють зміст відповідних понять, не розкривається і співвідношення між ними, що шкодить як нормотворчій, так і правозастосовній та інтерпретаційно-правовій діяльності. Зважаючи на прагнення України набути членства в Європейському Союзі, доцільно у вітчизняному законодавстві оперувати поняттями «кіберпростір» та «кібербезпека, що більшою мірою відповідає європейському підходу до правового регулювання відповідних відносин.

Тож держави вимушені виокремлювати в рамках політики національної безпеки такий її підвид, як кібербезпеку, а також вдаватися до формування відповідних структурних підрозділів в органах безпеки.

Попри те, що тематика кібербезпеки в Україні все частіше артикулюється на найвищому державному рівні, наукові дослідження, а також реальні заходи в цій сфері все ще залишаються багато в чому фрагментарними та несистемними [26, с. 120] і далеко не завжди враховують підходи Європейського Союзу в питаннях запровадження правової відповідальності за кіберзлочини.

Аналіз останніх досліджень і публікацій. Проблематика кібербезпеки привертає значну увагу науковців з кінця XX ст. Дослідження в цій сфері традиційно мають міждисциплінарний характер. До наукових розвідок, присвячених правовим проблемам кібербезпеки, можна віднести публікації зарубіжних (H. Bruijn [8], K. E. Eichensehr [27], U. Gorham-Oscilowski [32], P. T. Jaeger [32], J. Jang-Jaccard [34], M. Janssen [8], C. Leuprecht [40], S. Nepal [34], D. C. Schleher) [51] і вітчизняних (О. А. Баранов [3], Д. В. Дубов [26], Б. А. Кормич [37], В. А. Ліпкан [47]) авторів.

Мета та завдання дослідження. Метою статті є визначення ключових стратегічних проблем і шляхів їх вирішення задля розбудови ефективних механізмів забезпечення кібербезпеки в частині протидії злочинам фішингу. Відповідно до мети визначаються такі завдання: визначити типи та вплив кібератак; визначити фішинг як одну з найважливіших загроз кібербезпеки; проаналізувати таксономію різних типів фішингових атак та засобів захисту користувачів від них; визначити сучасні підходи Європейського Союзу в питанні запровадження кримінальної відповідальності за фішинг; підвищити рівень обізнаності громадськості у питаннях кримінально-правової ідентифікації фішингу.

Виклад основного матеріалу. Вибух інформаційних технологій стрімко змінює всі аспекти сучасного соціального, політичного, культурного та економічного життя. Глобальне медіа-агентство We Are Social та розробники платформи для управління соціальними мережами Hoot Suite на початку 2019 р. представили звіти, відповідно до яких наприкінці 2018 р. користувачами інтернету були 4,021 млрд осіб (53 % від населення планети), тоді як в 2015 р. доступ до Мережі мали 3,2 млрд людей (43 %), а в 1995 р. цей показник становив лише 1 % [52]. В Україні інтернет-аудиторія в 2018 р. становила 70% від населення (лише за 2018 р. вона зросла на 11 %) [57].

Аналіз, проведений на замовлення агентства Culumus Media в 2019 р., демонструє вражаючі обсяги інформації, що транслюються з соціальних мереж, e-commerce-сайтів, месенджерів та інших ресурсів в інтернеті кожну хвилину [49]. Зважаючи на отримані дані, а також позитивну динаміку зростання кількості користувачів інтернету, можна впевнено стверджувати, що людство стрімко просувається до формування дійсно глобального інформаційного суспільства. У такому суспільстві життя як окремого індивіда, так і різних соціальних груп, суспільства, держави і світу в цілому буде залежати від стану кіберпростору, його безпеки і надійності. Це пов'язано з тим, що відкритий та вільний

кіберпростір розширює свободу і можливості людей, збагачує суспільство, створює новий глобальний інтерактивний ринок ідей, досліджень та інновацій, стимулює відповідальну та ефективну роботу влади [59].

Однак глобальні технологічна та інформаційна революції, як і будь-які інші соціальні явища, окрім позитивного впливу на суспільний розвиток мають і зворотній бік – мова йде про їхні негативні наслідки, які породили чимало проблем і небажаних явищ та процесів. Йдеться не лише про виникнення глобального цифрового розриву між розвиненими країнами та рештою світу, який носить інтегральний характер і включає в себе розриви в економіці, освіті, рівні життя, доходах, харчуванні і т. ін. [29]. Не менш негативний, руйнівний характер мають кіберзлочинність, кібертероризм та інші явища, що становлять безпосередню загрозу національній безпеці держави [9]. Слід зазначити, що хоча кібербезпека є однією з найважливіших проблем, поінформованість громадськості щодо неї залишається обмеженою і поверховою.

Інтернет дав потужний поштовх для розвитку масової комунікації, торгівлі та обміну інформацією. Разом з тим сьогодні він є тією сферою, де здійснюється чимало правопорушень. Знеособлений характер цифрової інфраструктури зробив крадіжку ідентичності природним і надзвичайно привабливим проєктом [60, с. 186]. Кіберзлочинці активно використовують різні засоби викрадення інформації, зокрема фішинг.

Питання фальшивої ідентичності в інтернеті – це стара проблема, яка досі не отримала універсально правового розв'язання попри те, що захист конфіденційності є ключовою політичною метою Ради Європи і Європейського Союзу (право на конфіденційність закріплено ст. 8 Європейської конвенції про права людини [28], статтями 7, 8 Хартії основних прав Європейського Союзу [10] та Директивами 95/46 / ЄС та 97/66 / ЄС) [18].

Онлайн-сервіси стали невід'ємною складовою нашого життя: вони суттєво спрощують доступ до інформації користувачам і зменшують експлуатаційні витрати надавачам послуг. Однак користування онлайн-сервісом потребує певного рівня технічних навичок, якими володіють далеко не усі користувачі Інтернету. Саме категорія таких неосвічених, наївних користувачів часто стає жертвою фішингу, який є одним з найбільш поширених злочинів в Інтернеті.

Фішинг («phishing») також відомий як «підробка бренда» («brand spoofing») або шахрайство з платіжними картами («carding»), – це відносно новий (порівняно з вірусними атаками і хакерством) різновид кіберзлочину, метою якого є викрадення шляхом застосування комбінації різних методів соціальної інженерії та підробки вебсайтів конфіденційної інформації економічного характеру (таких особистих даних, як ім'я, дата народження, адреса, номер телефону, номер страхового свідоцтва, номери кредитної і медичної карток, обліковий запис і паролі, інформація про банківський рахунок, номер посвідчення водія) для скоєння у подальшому крадіжок, шахрайства чи інших злочинів [60, с. 187; 61, с. 290; 41].

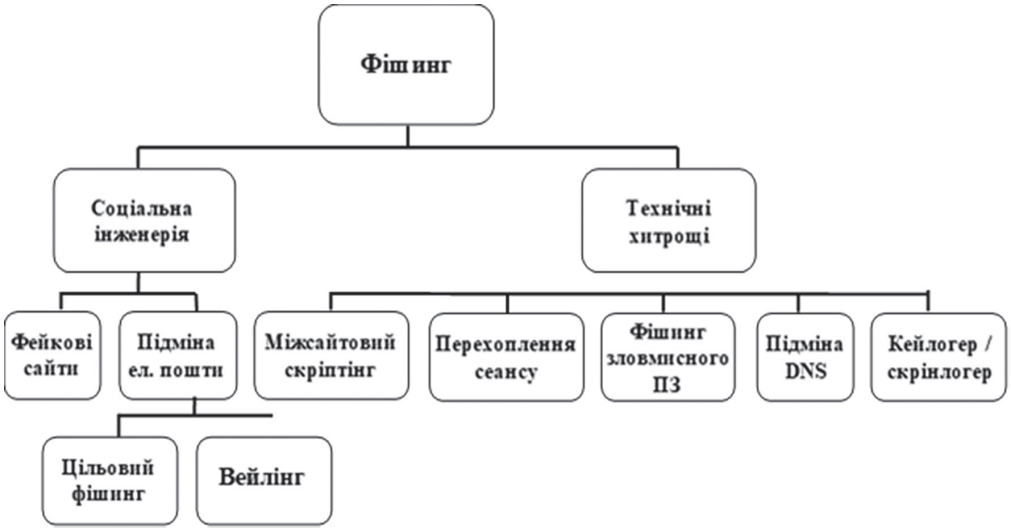

Рис. 1. Класифікація фішинг-атак [Наведено за: 33].

Небезпечність фішингу обумовлена передусім шкодою – він завдає пряму фінансову шкоду, а також породжує «кризу довіри»[1] до операцій в інтернеті, адже через суттєві втрати від фішинг-атак окремі фінансові інститути відмовляються від оплати і покладають відповідальність на клієнта [5], підриває маркетингові зусилля і загальний імідж компаній (на фінансові установи (банки та кредитні спілки) зазвичай спрямовано 60–80 % фішинг-атак), – яку він завдає електронній комерції, а також стрімким його поширенням унаслідок феноменальної прибутковості інвестицій у фішинг[2]. Існує думка, що за прибутковістю глобальна кіберзлочинність випереджає навіть торгівлю наркотиками [43, с. 41]. В окремих випадках фішинг-атаки можуть нести загрозу також національним інтересам[3], регіональній і міжнародній безпеці[4]. Також є ще один момент, який

[1] Загальновідомо, що довіра є визначальним фактором успіху електронного банкінгу [35; 30].

[2] Проведений аналіз засвідчує, що на відправку 10 000 000 електронних листів у місяць фішинг-шахраї витрачають 160 доларів. Навіть якщо на ці листи дадуть відповідь лише 0,001 % людей, прибуток шахраїв становитиме майже 125 000 доларів [53, с. 5].

[3] Так, під час президентської виборчої кампанії 2019 р. під удар фішинг-атак потрапили сервери та персональні комп'ютери співробітників ЦВК України. У липні 2017 р. зловмисники намагалися скомпрометувати робочі станції працівників на атомних електростанціях, розсилаючи націлені фішингові листи. У травні 2016 р. мала місце спроба фішингової атаки на поштові системи Християнсько-демократичного союзу — політичної партії Ангели Меркель. У березні 2016 р. під час президентської кампанії в США було «зламано» обліковий запис електронної пошти в Google голови виборчого штабу кандидата в президенти Х. Клінтон Дж. Подести.

[4] У березні 2020 р. масові фішинг-атаки були спрямовані на системи Всесвітньої організації охорони здоров'я (ВООЗ). Лише у Великій Британії шахраї на епідемії коронавірусу заробили 1 млн доларів. Шахраї видавали себе за співробітників Центру з контролю і профілактики захворювань або ВООЗ, використовуючи різні схеми – від доставки захисних масок до фішингових атак через електронну пошту. Було зареєстровано понад 4000 доменів, пов'язаних з коронавірусом. У березні 2018 р. Міністерство юстиції США висунуло підозру іранським хакерам, які

змушує говорити про небезпечність даного правопорушення, – кіберзлочини, зокрема фішинг, є різновидом організованої злочинності [7].

Пересічному інтернет-користувачу розпізнати фішинг-атаку буває досить складно через його довірливість[1] і погану обізнаність з методами і тактиками фішингу, які постійно оновлюються (спам дедалі частіше поєднується зі зловмисним програмним забезпеченням) [38].

Науковці Університету Карнегі Меллон (Carnegie Mellon University) встановили наступні причини вразливості людей до фішингу. По-перше, інтернет-користувачі схильні оцінювати законність вебсайту за його «зовнішнім виглядом», який шахраї легко дублюють. По-друге, багато користувачів не розуміють і не довіряють показникам безпеки у веббраузерах. По-третє, хоча деякі споживачі знають про фішинг, ця обізнаність не зменшує їх вразливості або не надає корисних стратегій для виявлення фішинг-атак. По-четверте, сприйняття серйозності наслідків фішингу не породжує належну поведінку користувачів [55; див. також: 23; 25; 62].

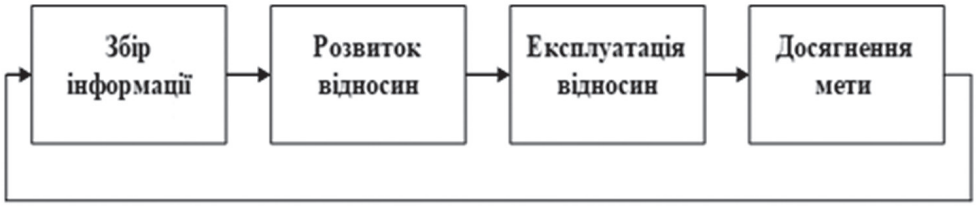

Рис. 2. Етапи фішинг-атак [Наведено за: 44].

Розрізняють чотири основні методи, що застосовуються фішерами.

«Dragnet Method», який передбачає використання спам-електронні листи, вебсайти, спливаючі вікна або підроблені рекламні банери з фальсифікованою корпоративною ідентифікацією (наприклад, товарні знаки, логотипи і фірмові найменування), які адресовані великій кількості людей (наприклад, клієнтам банку або членам організації конкретного сайт-аукціону). Цей метод не передбачає виявлення заздалегідь конкретних потенційних жертв, оскільки адресати беруться з випадкової бази даних.

«Rod-and-Reel method» (spear-phishing). Цільовий фішинг більш небезпечний, оскільки спрямований на конкретну цільову жертву (використовує

розіслали фішингові листи понад ста тисячам науковців по всьому світу. Жертвами атаки стали понад 140 університетів та 30 компаній в США, та 176 університетів у 21 іншій країні. У американських установ було викрадено близько 31 терабайта даних, вартістю близько 3,4 млрд доларів.

[1] Аналіз взаємозв'язку між демографією та сприйнятливістю до фішингу свідчить про те, що жертвами фішингу частіше стають жінки, аніж чоловіки (чоловіки мають більше шансів правильно розрізнити фішинг та законні вебсайти, ніж жінки (75,5 % правильно проти 64,4 % правильно)), а молодь (18–25 р.) більш чутлива до фішингу, ніж інші вікові групи. Також потенційними жертвами фішингу є люди з вадами зору, оскільки вони виключно покладаються на слухові сигнали, отримані від екранного зчитувача [55; 56].

людський фактор, здатність людини приймати необдумані і спонтанні рішення), стосовно якої спеціально збирається інформація аби зробити адресоване їй послання більш переконливим. Структура даного фішингу більш складна і складається з таких послідовних кроків: 1) планування (проведення розвідки, аналіз вразливості, вибір хитрощів); 2) підготовка (складання листа, розробка засобів атаки); 3) атака (відправка листа, впровадження шкідливого ПЗ); 4) збір (збір інформації шкідливим ПЗ, отримання і аналіз інформації); 5) шахрайство (використання інформації, продаж інформації, шантаж); 6) завершення (ліквідація доказів, позбавлення переслідувачів, оцінка ефективності) [63, с. 99].

«Lobsterpot Method». Він полягає у створенні вебсайтів, схожих на законні корпоративні вебсайти, які вузько визначають клас жертв фішерами. Менший клас потенційних жертв визначений заздалегідь, але не викликає реакції жертви. Достатньо того, що потерпілий сприйняв підроблений вебсайт як легальний і надав інформацію про особисті дані. У рамках цього методу підробка відбувається на рівні протоколу. Мета шахрая полягає або в отриманні доступу до захищеного сайту, або в маскуванні його справжньої особи. При цьому шахрай може викрасти адресу жертви, фальсифікуючи інформацію про маршрутизацію повідомлення, щоб здавалося, що воно прийшло з акаунта жертви замість його власного [50].

«Gillnet phishing Method». На відміну від попередніх методів «Gillnet phishing» меншою мірою зорієнтований на соціальну інженерію. Фішери вводять шкідливий код в електронні листи та вебсайти.

Розмірковуючи над програмою захисту від фішинг-атак, слід зазначити, що зосередження уваги лише на технічному оснащенні системи захисту інформації є помилкою, оскільки успішність даних злочинів обумовлена насамперед людським фактором. Хоча у науковій літературі наведено численні технічні рішення щодо попередження та нейтралізації фішинг-атак, слід погодитися з тим, що жодне із запропонованих рішень не стало «срібною кулею» у боротьбі проти фішингу [54].

Серед заходів, спрямованих на захист від фішинг-атак, передусім слід вказати на заходи організаційного характеру, які повинні бути спрямовані зокрема на навчання користувачів, підвищення їхньої обізнаності. На необхідності запровадження громадської інформаційно-просвітницької кампанії та пропаганді кращих практик у сфері кібербезпеки Європейська Рада наголошувала ще в 2001 р. [13]. Дана рекомендація залишається актуальною та практично значущою і сьогодні. У регламенті ЄС 2019/881 наголошується, що створене в 2004 р. Європейське агентство з мережевої та інформаційної безпеки (ENISA) має регулярно проводити просвітницькі та публічні освітні кампанії, спрямовані на кінцевих користувачів[1], тим самим сприяючи більш безпечній поведінці людей в інтернеті та їхній цифровій грамотності, підвищенню обізнаності про потенційні кіберзагрози, включаючи такі онлайн-злочини, як фішинг-атаки,

[1] Контекстуальне навчання, тренінги та інтерактивні ігри покращують здатність користувачів уникати фішинг-атак [39].

ботнети, фінансові та банківські шахрайства, випадки шахрайства з даними, а також сприяти багатофакторній автентифікації, анонімності та захисту даних (п. 40 Регламенту) [48].

При організації просвітницьких заходів слід зважати на те, що у світі налічується не менше 2,2 млрд осіб з порушенням зору або сліпоти. У цьому зв'язку особливої актуальності набуває проблема забезпечення доступності засобів антифішингу для людей із вадами зору для взаємодії з цими інструментами.

Проблема кіберзлочинності виглядає сьогодні набагато серйознішою, аніж це інколи здається, оскільки вона носить транскордонний характер. Спроба окремих держав запровадити кримінальне покарання за фішинг на національному рівні не вирішує проблему, оскільки для фішерів, які працюють по всьому світу, нескладно оминути національні бар'єри. Саме тому протидія кіберзлочинності потребує значних зусиль не лише окремих держав, але й міжнародних організацій (Європейського Союзу, Ради Європи, Інтерполу та ін.), які здатні забезпечити координацію спільних зусиль держав з розробки відповідного законодавства, ведення багатосторонніх переговорів з питань співробітництва, обміну інформацією і доказами, розслідування, конфіскації активів, консультацій з приводу політики, технічної допомоги, матеріально-технічного забезпечення тощо [1; 4; 5].

Існують певні проблеми щодо запровадження кримінально-правової відповідальності за фішинг-атаки, оскільки фішинг взагалі не є окремим злочином відповідно до матеріального кримінального права[1]. Це певне «парасолькове» поняття, яке охоплює низку розпочатих чи завершених злочинів [36]. Фішинг-атаки з точки зору кримінального права можуть відповідати різним категоріям злочинів (вимагання, шахрайство, шантаж, правопорушення, що пов'язані з обробкою персональних даних).

Співробітництво держав на міжнародному рівні з питань протидії кіберзлочинності розпочалося наприкінці XX ст. 9–10 грудня 1997 р. під час роботи саміту G8 на рівні міністрів юстиції і внутрішніх справ у Вашингтоні було сформульовано спільну позицію держав-учасниць, яку викладено у комюніке щодо Плану боротьби зі злочинами у сфері високих технологій [14]. Того ж року було створено форум з інтернет-злочинності, учасниками якого були співробітники поліції, міністерств внутрішніх справ і захисту даних, представники інтернет-індустрії.

Перші кроки на шляху формування Європейським Союзом власної політики в сфері забезпечення мережевої та інформаційної безпеки (всебічної стратегії безпеки електронних мереж, включаючи практичні заходи щодо впро-

[1] Сьогодні лідером у правовій протидії фішингу є США, антифішингове законодавство яких формувалося на початку XXI ст. Двадцять три штати і Гуам мають закони, що спеціально спрямовані на фішингові схеми. В інших штатах діють закони, що стосуються комп'ютерних злочинів, шахрайських дій або крадіжки особистих даних, які також можуть застосовуватися до фішингових злочинів. США, як і інші країни, зіткнулися з криміналізацією даного злочину, оскільки проблема фішингу має здебільшого вирішуватися технологічними засобами, аніж правовими [58].

вадження) було зроблено в 2001–2002 рр. Європейською Радою, Радою ЄС, Європейською Комісією та Європейським Парламентом у зв'язку з тим, що на рівні Союзу не відбувався процес зближення кримінального права в цій сфері, що породжувало проблеми із розслідуванням кіберзлочинів. Така ситуація вочевидь не стримує тих, хто планує злочини в кіберпросторі. Було визнано за необхідне поширити кримінальне законодавство держав-членів на дії, що призводять до несанкціонованого доступу до комп'ютерних мереж, зокрема до порушення безпеки особистих даних [13; 17].

У 2001 р. Європейська Рада доручила Європейській Комісії розробити перелік національних заходів, зокрема Комісія мала сформулювати пропозиції щодо законодавства ЄС в сфері кіберзлочинності [13]. Було також створено форум ЄС, в рамках якого мали відбуватися дискусії між правоохоронними органами, промисловцями, інтернет-провайдерами, операторами зв'язку, громадськими організаціями, представниками споживачів, органами захисту даних та іншими зацікавленими суб'єктами з метою пошуку оптимального балансу між захистом основних прав і свобод людини, зокрема права на недоторканність приватного життя, необхідністю боротьби з кіберзлочинністю і фінансовим тягарем, що покладається на постачальників послуг [12].

Однак суттєвого прогресу в цьому напрямі не було досягнуто, і в 2005 р. Рада ЄС вимушена була звернути увагу на те, що суттєві прогалини та розбіжності в кримінальному законодавстві держав-членів перешкоджають боротьбі з кіберзлочинністю та ускладнюють ефективне співробітництво поліції та судів у сфері нападів на інформаційні системи [16]. Попри усвідомлення необхідності уніфікації кримінального законодавства в частині протидії кіберзлочинності реального прогресу в цьому напрямі Європейський Союз так і не досягнув (див. Звіт Європейської Комісії про шахрайство щодо безготівкових платіжних засобів в ЄС: виконання Плану дій 2004–2007 років [11]), на що вказує Директива ЄС 2019/713, в пункті 13 якої зазначено, що потрібен загальний кримінально-правовий підхід щодо складових елементів злочинної поведінки, які сприяють або готують шлях до фактичного шахрайського використання безготівкового платіжного засобу. У даній Директиві європейський законодавець не обмежується лише постановкою загальної мети. Директива вимагає, по-перше, використання кримінального законодавства для надання правового захисту платіжним інструментам, в яких використовуються спеціальні форми захисту від імітації або зловживання, з метою спонукання операторів надавати такі спеціальні форми захисту для випущених ними платіжних інструментів (п. 12)[1], по-друге, пропонує розуміти під поняттям «злочинна поведінка» також

[1] Дану вимогу було закріплено ще раніше у Директиві ЄС 2016/1148 (вимога, адресована усім державам-членам щодо наявності мінімальних можливостей та стратегій, що забезпечують високий рівень безпеки мережевих та інформаційних систем на їхній території., а також вимоги до операторів основних послуг та до постачальників цифрових послуг, щоб сприяти культурі управління ризиками та забезпечити повідомлення про найбільш серйозні випадки) [21] та у п. 96 Директиви ЄС 2015/2366: для обмеження ризиків, пов'язаних із фішинг та іншими шахрайськими діями, необхідно безпечне використання персоналізованих даних щодо безпеки.

поведінку, спрямовану на збирання та володіння платіжними інструментами з наміром вчиняти шахрайство, наприклад, шляхом фішингу, скімінгу або спрямування чи перенаправлення користувачів платіжних послуг на імітаційні вебсайти та їх розповсюдження, наприклад, шляхом продажу інформації про кредитні картки в Інтернеті (п. 13), і, по-третє, стосовно кримінальних злочинів, зазначених у Директиві, поняття умислу застосовується до всіх елементів, що складають ці кримінальні правопорушення відповідно до національного законодавства; умисний характер діяння, а також будь-які знання або цілі, що необхідні як елемент правопорушення, можуть бути виключені з об'єктивних фактичних обставин; кримінальні злочини, які не потребують умислу, не охоплюються цією Директивою (п. 12) [22].

Приклади антифішингового законодавства [Наведено за: 6, с. 557]

Типи антифішингових законів	**Приклади антифішингових законів**
Законодавство, яке перешкоджає поширенню фішинг-повідомлень	Controlling the Assault of Non-Solicited Pornography And Marketing (CAN-SPAM) Act of 2003, USA; Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data; Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications);
Законодавство, що забороняє фальшиві вебсайти	Copyright Ordinance (Cap 528) of Hong Kong; Wire Fraud Act in the U.S. (18 U.S.C. § 1343); Convention on Cybercrime (Offences related to infringements of copyright and related rights, Article 10).
Законодавство, що спрямоване на збереження конфіденційних даних	Personal Data (Privacy) Ordinance (Cap. 486) of Hong Kong; Directive (EU) 2018/1972 of the European Parliament and of the Council of 11 December 2018 establishing the European Electronic Communications Code (Recast); Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications); Convention on Cybercrime (Data Interference, Article 4); Convention on Cybercrime (System interference, Article 5).

У цьому відношенні користувач повинен мати можливість покладатися на прийняття заходів, що захищають конфіденційність та цілісність персоналізованих даних безпеки [20].

Типи антифішингових законів	Приклади антифішингових законів
Законодавство, що стримує крадіжку ідентичності	Crime Ordinance (Cap. 200) of Hong Kong; Identity Theft and Assumption Deterrence Act, which amended Title 18, U.S. Code, Section 1028, 1998; Identity Theft Penalty Enhancement Act, 2004; 18 U.S. Code § 1029. Fraud and related activity in connection with access devices; 18 U.S.C. § 1344 – U.S. Code – Unannotated Title 18. Crimes and Criminal Procedure § 1344. Bank fraud; Computer fraud (18 U.S.C. § 1030(a)(4)) (US); Convention on Cybercrime (Computer-related fraud, Article 8).

Хоча потреба в уніфікації кримінального законодавства держав-членів у сфері кібербезпеки визнана на рівні законодавства ЄС, слід зауважити, що її реалізація на національному і наднаціональному рівні відбувається надзвичайно повільно [45].

Висновки. Отже, фішинг – одна з найбільш серйозних загроз кібербезпеки сучасності, що полягає насамперед у заподіянні фінансової шкоди окремим користувачам і організаціям, а також може становити загрозу національній та міжнародній безпеці.

Через складний характер фішинг-атак не існує єдиної універсальної моделі виявлення усіх можливих категорій загроз. Саме тому існує нагальна потреба у розробці моделей, які б застосовували декілька фільтрів для виявлення фішингових сайтів і давали підказки щодо реального сайту. Важливо, щоб інтерфейс таких моделей був настільки доступний, що широке коло користувачів, насамперед люди з вадами зору, могли їх ефективно використовувати.

Сучасна злочинність постійно та невпинно трансформується, тож перед державою постають все нові й нові виклики, які потребують організаційного, правового та технічного втручання з метою превентивного захисту кіберпростору, банківської системи та критичної інфраструктури. У сучасному глобалізованому світі проблема організованої злочинності не може бути вирішена без правових контрзаходів і норм міжнародного права. Сучасний стан національної безпеки потребує вдосконалення національного законодавства, його узгодження з міжнародними стандартами. Тільки у тісній взаємодії з міжнародними організаціями, зокрема Європейським Союзом, можливо забезпечити захист інформаційного простору від кібератак та кібертероризму.

References

1. Alexander, R. (1998). EU: The EC Money Laundering Directive. *Journal of Money Laundering Control, Vol. 2*.

2. Antonelli, C., Geuna, A., Steinmueller, W.E. (2000). Information and Communication Technologies and the Production, Distribution and Use of Knowledge. *International Journal of Technology Management, Vol. 20 (1–2), 72–94*.

3. Baranov, O.A. (2014). Pravove zabezpechennia informatsiinoi sfery: teoriia, metodolohiia i praktyka. Kyiv: Edelveis.

4. Bell, R.E. (2002). An Introductory: Who is Who for Money Laundering Investigators. *Journal of Money Laundering Control, Vol. 5, 287–295.*

5. Birk, D., Gajek, S., Grobert, F., Sadeghi, Ah.-R. (2007). Phishing Phishers—Observing and Tracing Organized Cybercrime. Second International Conference on Internet Monitoring and Protection. URL: https://www.academia.edu/34821911/Phishing_Phishers_-_Observing_and_Tracing_Organized_Cybercrime.

6. Bose, I. (2007). Unveiling the Mask of Phishing: Threats, Preventive Measures, and Responsibilities. *Communications of the Association for Information Systems, Vol. 19, 544–566.*

7. Brenner, S. (2002). Organized Cybercrime? How Cyberspace May Affect the Structure of Criminal Relationships. *North Carolina Journal of Law and Technology, Vol. 4.*

8. Bruijn, H. de, Janssen, M. (2017). Building cybersecurity awareness: The need for evidence-based framing strategies. *Government Information Quarterly, Vol. 34, Issue 1, 1–7.* doi: https://doi.org/10.1016/j.giq.2017.02.007.

9. Chang, M., Kuhn, R., Weil, T. (2018). Cyberthreats and Security. *IT Professional, 3, 20–22.*

10. Charter of Fundamental Rights of the European Union (2000/C 364/01). *Official Journal of the European Communities. C 364 of 18.12.2000.*

11. Commission staff working document – Report on fraud regarding non cash means of payments in the EU: the implementation of the 2004–2007 – EU action plan. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1585384025208&uri=CELEX:52008SC0511.

12. Communication from the Commission to the Council, the European Parliament, the Economic and Social Committee and the Committee of the Regions. Creating a Safer Information Society by Improving the Security of Information Infrastructures and Combating Computer-related Crime. Brussels, 26.01.2001 COM (2000). 890 final. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52000DC0890&from=EN.

13. Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions – Network and Information Security: Proposal for A European Policy Approach. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52001DC0298.

14. Communique Meeting of Justice and Interior Ministers of The Eight, Washington, D.C. 10 December, 1997. URL: https://www.justice.gov/sites/default/files/ag/legacy/2004/06/08/97Communique.pdf.

15. Copeland, Th.E. (2000). The Information Revolution and National Security. URL: https://www.files.ethz.ch/isn/104586/Information_Revolution_National_Security.pdf.

16. Council Framework Decision 2005/222/JHA of 24 February 2005 on attacks against information systems. *Official Journal of the European Union, L 69, 16.03.2005, 67–71.*

17. Council Resolution of 28 January 2002 on a common approach and specific actions in the area of network and information security. *Official Journal of the European Union, C 43, 16.02.2002, 2–4.*

18. Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. *Official Journal, L 281, 23/11/1995, 0031–0050.*

19. Directive 97/66/EC of the European Parliament and of the Council of 15 December 1997 concerning the processing of personal data and the protection of privacy in the telecommunications sector. *Official Journal, L 024, 30/01/1998, 0001–0008.*

20. Directive 2015/2366/EC of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC. *Official Journal of the European Union, L 337, 23.12.2015, 35–127.*

21. Directive 2016/1148/EC of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union. *Official Journal of the European Union, L 194, 19.07.2016, 1–30.*

22. Directive 2019/713/EC of the European Parliament and of the Council of 17 April 2019 on combating fraud and counterfeiting of non-cash means of payment and replacing Council Framework Decision 2001/413/JHA. *Official Journal of the European Union, L 123, 10.05.2019, 18–29.*

23. Dhamija, R., Tygar, J.D., Hearst, M. (2006). Why phishing works. *In Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (Montréal, Québec, Canada, April 22–27, 2006). R. Grinter, T. Rodden, P. Aoki, E. Cutrell, R. Jeffries, and G. Olson (Eds.). CHI '06. ACM Press, New York, NY, 581–590.

24. Doktryna informatsiinoi bezpeky Ukrainy: zatverdzhena Ukazom Prezydenta Ukrainy vid 25 liutoho 2017 r. № 47/2017. URL: https://zakon.rada.gov.ua/laws/show/47/2017.

25. Downs, J.S., Holbrook, M., Cranor, L.F. (2007). Behavioral response to phishing risk. *In Proceedings of the Anti-Phishing Working Groups 2nd Annual Ecrime Researchers Summit* (Pittsburgh, Pennsylvania, October 04–05, 2007). *eCrime '07, vol. 269.* ACM, New York, NY, *37–44.*

26. Dubov, D.V. (2013). Stratehichni aspekty kiberbezpeky Ukrainy. *Stratehichni priorytety, 4, 119–127.*

27. Eichensehr, K.E. (2016). Public-private cybersecurity. *Texas Law Review, Vol. 95, 467–538.*

28. European Convention on Human Rights as amended by Protocols Nos. 11 and 14 supplemented by Protocols Nos. 1, 4, 6, 7, 12, 13 and 16. URL: https://www.echr.coe.int/Documents/Convention_ENG.pdf.

29. Elyakov, A. (2003). Oborotnaya storona informacionnoj revolyucii. *Vysshee obrazovanie, 3, 82–87.*

30. Gefen, D. (2002) Reflections on the Dimensions of Trust and Trustworthiness Among Online Consumers. *ACM SIGMIS Database, Vol. 33, 3, 38–53.*

31. Goodman, M.D., Brenner, S.W. (2002). The emerging consensus on criminal conduct in cyberspace. *International Journal of Law Infomation Technology, Vol. 10, 139–223.*

32. Gorham-Oscilowski, U., & Jaeger, P.T. (2008). National Security Letters, the USA PATRIOT Act, and the Constitution: The tensions between national security and civil rights. *Government Information Quarterly, 25, 625–644.* doi 10.1016/j.giq.2008.02.001.

33. Gupta, B.B., Arachchilage, N.A.G., Psannis, K.E. (2018). Defending against Phishing Attacks: Taxonomy of Methods, Current Issues and Future Directions. *Telecommunication Systems, vol. 67, 247–267.*

34. Jang-Jaccard, J., Nepal, S. (2014). A survey of emerging threats in cybersecurity. *Journal of Computer and System Sciences, Vol. 80, Issue 5, 973–993.*

35. Kautonen, T., Karjaluoto, H. (2008). Trust and New Technologies: Marketing and Management on the Internet and Mobile Media. Cheltenham: Edward Elgar Publishing.

36. Kikerpill, K., Siibak, A. (2019). Living in a Spamster's Paradise: Deceit and Threats in Phishing Emails. *Masaryk University Journal of Law and Technology, Vol. 13:1, 45–66.* doi: 10.5817/MUJLT2019-1-3.

37. Kormych, B.A. (2003). Orhanizatsiino-pravovi zasady polityky informatsiinoi bezpeky Ukrainy. Odesa: Yurydychna literatura.

38. Kumar, A., Chatterjee, J.M., Díaz, V.G. (2020). A novel hybrid approach of SVM combined with NLP and probabilistic neural network for email phishing. *International Journal of Electrical and Computer Engineering (IJECE), Vol. 10, 1, 486–493.* doi: 10.11591/ijece.v10i1.

39. Kumaraguru, P., Rhee, Y., Acquisti, A., Cranor, L., Hong, J., Nunge, E. (2007). Protecting People from Phishing: The Design and Evaluation of an Embedded Training Email System. In Proceedings of the 2007 Computer Human Interaction, CHI.

40. Leuprecht, C., et al. (2016). Beyond the Castle Model of cyber-risk and cyber-security. *Government Information Quarterly. Vol. 33 (2), 250–257.* doi: http://dx.doi.org/10.1016/j.giq.2016.01.012.

41. Manap, N.A., Rahim, A.A., Taji, H. (2015). Cyberspace Identity Theft: An Overview. *Mediterranean Journal of Social Sciences, Vol. 6, 4 S3, 290–299.* doi: 10.5901/mjss.2015.v6n4s3p290.

42. Mansell, R. (2010). The life and times of the information society. *Prometheus. Vol. 28 (2), 165–186.* doi: 10.1080/08109028.2010.503120.

43. McCombie, S., Pieprzyk, J., Watters, P. (2009). Cybercrime Attribution: An Eastern European Case Study. Proceedings of the 7th Australian Digital Forensics Conference. *41–51*. URL: https://eprints.qut.edu.au/73391/1/73391.pdf.

44. Mitnick, K. & Simon, W. (2002). The art of deception: Controlling the human element of security. New York, New York: Wiley Publishing.

45. Moisea, A.C. (2017). Considerations of Criminal Law and Forensic Science Regarding the Illegal Access to a Computer System. *AGORA International Journal of JuridicalSciences, 2, 49–57*.

46. Mustafa, H. Digital Social Engineering Threatens Cybersecurity. *International Journal of Innovative Technology and Exploring Engineering (IJITEE), Vol. 9, Issue 1, 4016–4025*.

47. Lipkan, V.A. (Ed.). (2015). Pravovi zasady rozvytku informatsiinoho suspilstva v Ukraini. Kyiv: FOP Lipkan O. S.

48. Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act). *Official Journal of the European Union, L 151, 07.06.2019, 15–69*.

49. Rossokhyna, V. Chto proyskhodyt v ynternete za mynutu: ynfohrafyka. URL: https://www.likeni.ru/analytics/chto-proiskhodit-v-internete-za-minutu-infografika.

50. Rusch, J. (2005). The compleat cyber-angler: A guide to phishing. *Computer Fraud & Security, (1):4-6*. doi: 10.1016/S1361-3723(05)00145-4.

51. Schleher, D.C. (1999). Electronic warfare in the information age. Norwood: Artech House Publishers.

52. Serheeva, Yu. (2018). Internet 2017–2018 v myre y v Rossyy: statystyka y trendy. URL: https://www.web-canape.ru/business/internet-2017-2018-v-mire-i-v-rossii-statistika-i-trendy.

53. Singh, N.P. (2007). Online Frauds in Banks with Phishing. *Journal of Internet Banking and Commerce, Vol. 12(2), 1–27*.

54. Shaikh, A.N., Shabut, A.M., Hossain, M.A. (2016). A literature review on phishing crime, prevention review and investigation of gaps. 10th International Conference on Software, Knowledge, Information Management & Applications (SKIMA). URL: https://www.researchgate.net/publication/316722080_A_literature_review_on_phishing_crime_prevention_review_and_investigation_of_gaps. DOI: 10.1109/SKIMA.2016.7916190.

55. Sheng, St., Holbrook, M., Kumaraguru, P., Cranor, L. (2010). Who Falls for Phish? A Demographic Analysis of Phishing Susceptibility and Effectiveness of Interventions. Conference: Proceedings of the 28th International Conference on Human Factors in Computing Systems, CHI 2010, Atlanta, Georgia, USA, April 10–15, *373–382*. URL: https://www.researchgate.net/publication/221514257_Who_falls_for_phish_A_demographic_analysis_of_phishing_susceptibility_and_effectiveness_of_interventions. DOI: 10.1145/1753326.1753383.

56. Sonowal, G., Kuppusamy, K.S. (2020). PhiDMA – A phishing detection model with multi-filter approach. *Journal of King Saud University – Computer and Information Sciences, Vol. 32, Issue 1, 99–112*. doi: https://doi.org/10.1016/j.jksuci.2017.07.005.

57. Statistika internet-auditorii Ukrainy i ispolzuemyh ustrojstv. URL: https://seoukraine.com.ua/statistika-internet-auditorii-ukrainy-i-ispolzuemyh-ustroystv.

58. Stevenson, R.L.B. (2005). Plugging the «Phishing» Hole: Legislation Versus Technology. *Duke Law & Technology Review, № 5*. URL: https://scholarship.law.duke.edu/cgi/viewcontent.cgi?article=1126&context=dltr.

59. Stratehiia kiberbezpeky Ukrainy: zatverdzhena Ukazom Prezydenta Ukrainy vid 15 bereznia 2016 r. № 96/2016. URL: https://zakon.rada.gov.ua/laws/show/96/2016#n11.

60. Verma, A. (2013). Effects of Phishing on E-Commerce with Special Reference to India. Interdisciplinary Perspectives on Business Convergence, Computing, and Legality (Advances in E-Business Research), *186–197*. URL: http://pdfs.semanticscholar.org/9208/138fe9698717e5096cc93430337aeab80cb9.pdf. doi: 10.4018/978-1-4666-4209-6.ch017.

61. What's phishing? How to be safe? URL: http://inhome.rediff.com/money/2004/dec/20spec.htm.

62. Wu, M., Miller, R.C., Garfinkel, S.L. (2006). Do security toolbars actually prevent phishing attacks?. In Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (Montréal, Québec, Canada, April 22227, 2006). R. Grinter, T. Rodden, P. Aoki, E. Cutrell, R. Jeffries, and G. Olson (Eds.). CHI '06. ACM Press, New York, NY, *601–610*.

63. Zhurin, S.I., Komarkov, D.E. (2018). Zashita vneshnego informacionnogo perimetra organizacii ot celevogo fishinga. *Bezopasnost informacionnyh tehnologij=ITSecurity, Vol. 25, 4, 96–108* [in Russian].

Yakoviyk I. V., Doctor of Law, Full Professor, Head of the European Union Law Department, Yaroslav Mudryi National Law University, Ukraine, Kharkiv.
e-mail: yakoviyk@ukr.net ; ORCID 0000-0002-8070-1645

Voloshyn A. P., Postgraduate Student of the European Union Law Department, Yaroslav Mudryi National Law University, Ukraine, Kharkiv.
e-mail: voloshyn8888@gmail.com ; ORCID 0000-0002-3600-3778

Shovkun A. A., Master of the Security Service of Ukraine Legal Training Institute, Yaroslav Mudryi National Law University, Ukraine, Kharkiv.
e-mail: toni.shovkun@gmail.com ; ORCID 0000-0002-5280-8066

Legal aspects of counteracting phishing: the European Union experience

Cybersecurity is increasingly seen as a fundamental problem of the state, which comprehensively affects its security and defense, economy, certain spheres of public life, in particular energy, health care and others. Reliable operation of data networks, computer systems and mobile devices is a prerequisite for the effective state and society functioning, an individual's life. The reliability of key public information systems depends on many factors: cyberattacks, hardware and software failures, and all kinds of errors. The significant increase in the number of incidents in cyberspace necessitates a systematic analysis of sources of threats, the first place among which is phishing. The introduction of criminal responsibility for phishing is complicated by the fact that "phishing" is an "umbrella" concept that covers a number of launched or committed crimes. From criminal law point of view, phishing attacks can correspond to different categories of crimes (extortion, fraud, blackmail, offenses related to the processing of personal data, etc.). The attempt by some states to impose criminal penalties for phishing at the national level does not solve the problem, since it is not difficult for phishers who work worldwide to cross national barriers. That is still the reason why counteracting cybercrime requires significant efforts not only by individual states but also by international organizations, in particular by the European Union.

Keywords: cyberspace; cybersecurity; cybercrime; online fraud; phishing; anti-phishing tools; criminal law; European Union.

Рекомендоване цитування: Яковюк І. В., Волошин А. П., Шовкун А. О. Правові аспекти протидії фішингу: досвід Європейського Союзу. *Проблеми законності*. 2020. Вип. 149. С. 8–23. doi: https://doi.org/10.21564/2414-990x.149.200028.

Suggested Citation: Yakoviyk, I.V., Voloshyn, A.P., Shovkun, A.A. (2020). Pravovi aspekty protydii fishynhu: dosvid Yevropeiskoho Soiuzu [Legal aspects of counteracting phishing: the European Union experience]. *Problemy zakonnosti – Problems of Legality, issue 149, 8–23*. doi: https://doi.org/10.21564/2414-990x.149.200028 [in Ukrainian].

Надійшла до редколегії 01.04.2020 р.